11-03-00 A

JC952 U.S. PTO 11/02/00

PTO/SB/05 (08-00)
Approved for use through 10/31/2002 OMB 0651-0032
U.S. Patent and Trademark Office, U S DEPARTMENT OF COMMERCE

Please type a plus sign (+) inside this box → ☐

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	ATI-000153BT
First Inventor	David I.J. Glen
Title	WRITE ONCE SYSTEM AND METHOD FOR FACILITATING DIGITAL ENCRYPTED TRANSMISSIONS
Express Mail Label No.	EL566349206US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Commissioner for Patents, Box Patent Application, Washington, DC 20231

1. [X] Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. [ ] Applicant claims small entity status. See 37 CFR 1.27.
3. [X] Specification [*Total Pages* 11] *(preferred arrangement set forth below)*
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. [X] Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 1]
5. Oath or Declaration [*Total Pages* 2]
   a. [X] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 CFR 1.63 (d)) *(for continuation/divisional with Box 17 completed)*
      i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [ ] Application Data Sheet. See 37 CFR 1.76
7. [ ] CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. [ ] CD-ROM or CD-R (2 copies); or
      ii. [ ] paper
   c. [ ] Statements verifying identity of above copies

JC926 U.S. PTO 09/704329 11/02/00

ACCOMPANYING APPLICATION PARTS

9. [X] Assignment Papers (cover sheet & document(s))
10. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* [ ] Power of Attorney
11. [ ] English Translation Document *(if applicable)*
12. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
13. [ ] Preliminary Amendment
14. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. [ ] Other. .....

17. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:*

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: _____/_____

Prior application information. *Examiner* _____ *Group / Art Unit* _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

18. CORRESPONDENCE ADDRESS

[X] *Customer Number or Bar Code Label* 25310 *(Insert Customer No. or Attach bar code label here)* or [ ] *Correspondence address below*

Name	Volpe and Koenig, P.C. DEPT ATI				
Address					
City		*State*		*Zip Code*	
Country		*Telephone*		*Fax*	

Name (Print/Type)	C. Frederick Koenig III, Esquire	*Registration No. (Attorney/Agent)*	29,662
Signature		*Date*	11/2/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Express Mail Label No. EL566349206US

Volpe and Koenig, P.C. Revision of PTO/SB/17 (08-00)
Approved for use through 10/31/2002. OMB 0651-0032
U S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT	($) 750.00

Complete if Known	
Application Number	Not Yet Known
Filing Date	Not Yet Known
First Named Inventor	David I. J. Glen
Examiner Name	Not Yet Known
Group Art Unit	Not Yet Known
Attorney Docket No.	ATI-000153BT

METHOD OF PAYMENT (check one)

1. [X] The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to

Deposit Account Number: 50-0441

Deposit Account Name: ATI Technologies Inc.

[X] Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

[ ] Applicant claims small entity status. See 37 CFR 1 27

2. [ ] **Payment Enclosed:**

[ ] Check [ ] Credit card [ ] Money Order [ ] Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	710.00
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 710.00

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below	Fee Paid
Total Claims	12 - 20** =	0	X 18.00	= 0
Independent Claims	2 - 3** =	0	X 80.00	= 0
Multiple Dependent				=

**or number previously paid, if greater; For Reissues, see below

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for *ex parte* reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	40.00
146	710	246	355	Filing a submission after final rejection (37 CFR § 1 129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 40.00

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	C. Frederick Koenig III, Esquire	Registration No (Attorney/Agent)	29,662	Telephone	215-568-6400
Signature				Date	November 2, 2000

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0 2 hours to complete Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO. Assistant Commissioner for Patents, Washington, DC 20231.

Express Mail Label No. EL566349206US

WRITE ONCE SYSTEM AND METHOD FOR FACILITATING DIGITAL ENCRYPTED TRANSMISSIONS

The present invention relates to a system and process for facilitating unique code encryption between a computer and an associated peripheral device. In particular, it relates to facilitating HDCP encryption or the like on a digital video interface card which digitally communicates with a digital display or monitor.

BACKGROUND

Digital display devices and other digital peripheral devices are well known in the art. Digital display devices can be designed with video signal inputs to accept either a direct digital signal and/or an analog signal which is converted to digital by the display device. Additionally, some analog display devices accept a digital video signal output.

One concern in the industry is the unauthorized of copying of copyrighted content which may be contained in a video signal. If a video signal is intercepted between transmission from a computer system to a peripheral device, such as a display, it can be used to make virtually identical copies of the video content without any degradation or loss of quality.

Some systems avoid this concern by having an analog output from the computer and an analog input to the digital display device so that only an analog signal may be intercepted. Although copies of the video content can be made based upon the analog signal, there is inherently some degradation and quality loss associated with such an analog signal which compounds when repeated copies are made using analog transmissions. However, where an analog signal is transmitted from the computer to the peripheral digital device, the signal received by the digital device is likely to be of a lower quality than if a digital signal were transmitted between the computer and the peripheral device.

In order to facilitate the transmission of digital signals from a computer to a digital peripheral device while inhibiting unauthorized content copying, encryption schemes and

protocols have been developed to encrypt the digital signal before transmission from the computer and then to decrypt the signal in the digital peripheral device. One proposed protocol is High bandwidth Digital Content Protection (HDCP) specification which requires a graphics controller to store a large set of encryption keys that are unique to the interface devices used to output an encrypted digital signal. Under HDCP, each interface device must be allocated its own unique encryption key data. Thus, each interface device or computer system must be individualized. This poses a manufacturing problem since it is more efficient to manufacture on a mass scale computer systems and/or interface cards which are identical.

It would be desirable to provide a computer system and/or interface device which can be easily mass produced, but which also can support encryption systems such as HDCP.

SUMMARY

A digital interface device is provided for facilitating key encryption of a digital signal which is communicated from a computer system to an associated peripheral device, such as a digital display device. The peripheral device decrypts the communicated digital signal during use.

The digital interface device may be built into the computer system or provided as a separate interface card. In either case, the resulting system has a digital output port, digital output formatting circuitry associated with the port and an electrically programmable non-volatile memory such as a flash RAM for storing a basic input/output system (BIOS) for, inter alia, controlling digital output formatting. The interface device is configured such that the non-volatile RAM has a specific addressable write-protectable area allocated for storing an encryption key flag at a flag address along with encryption key data. The write-protectable area being rendered read-only when a predetermined flag value is stored at the flag address. Thus, encryption key data may be stored in the specific write-protectable area of the non-volatile RAM in connection with storing the predetermined flag at that flag address such that encryption data cannot be altered when

the non-volatile RAM is subsequently written to, such as when a BIOS stored in the non-volatile RAM is updated or when an attempt is made to tamper with the encryption keys.

Preferably, the digital interface device is configured to receive either a first predetermined flag value in association with key encryption data which first flag value indicates encryption enablement or a second predetermined flag value which second flag value indicates encryption disablement, in which case the digital interface device is permanently disabled from using the key encryption. If neither of the predetermined flags are contained at the flag address, the write-protectable area of the non-volatile RAM is writable to receive either the first flag value with encryption data or the disabling second flag value.

Preferably, the digital peripheral device is a digital display and the digital output port is configured to output a digital video signal. Also, it is preferred to configure the digital interface device as a digital video interface card, but the interface can be directly incorporated into a computer system's motherboard or other configuration which does not require a separate interface card.

The specific area for storing the encryption key flag and data is preferably at least 1k bytes and is preferably located as an address range higher than an address range reserved for a BIOS in the non-volatile RAM.

As a result of the invention, identical interface cards or systems can be mass-produced and thereafter be uniquely enabled or disabled from using a digital encryption system such as HDCP in an efficient cost-effective manner.

BRIEF DESCRIPTION OF THE DRAWINGS

The above, as well as other objects of the present invention will become apparent when reading the accompanying description and drawings in which:

Figure 1 is a schematic diagram of a computer and an associated digital display device which uses the digital interface of the present invention.

Figure 2 is a schematic diagram of the digital interface in a preferred add-in card embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to Figure 1, a computer system is illustrated having a computer 10 coupled with an associated digital peripheral device, such as digital display device 12. The computer 10 includes a digital video output port 14 which is coupled to a digital signal input port 16 of the digital display device 12 via conventional means such as a cable 18. The digital video signal output 14 is controlled by a digital interface device 20 such as an add-in card as illustrated in Figure 2. The digital interface device may also include an analog port 22 so that the computer may output video signals either in digital or analog.

The digital interface device or card 20, includes graphic control circuitry 24 typically embodied in a chip known as a graphics controller. In the add-in card embodiment of the interface device 20, the graphics controlling circuitry 24 typically receives and communicates with the rest of the computer 10 via an edge card connector 28 which is typically received in an appropriate slot on a motherboard of the computer 10.

The graphics controller circuitry 24 is controlled by a basic input/output system program (BIOS) which is stored in a non-volatile RAM 26 of the interface device 20. The non-volatile RAM 26 is a conventional semi-conductor chip device which retains its memory when powered off. During normal video display operations, the non-volatile RAM acts as a read-only memory (ROM) providing the graphic control circuitry 24 with programming instructions such as, for example, the formatting of the graphic output signals. From time to time, it is desirable to upgrade the BIOS which is accomplished by writing the updated BIOS into the non-volatile RAM 26. This update operation can be controlled by the graphic control circuitry 24.

In order to inhibit the unauthorized copying of the digital signal passed through the connecting cable 18, that digital signal may be encrypted. Accordingly, the interface device is designed so that it may optionally be configured to use a proprietary encryption scheme such as HDCP. Under HDCP, the digital interface device must contain unique encryption key data which is not subject to tampering. However, it is often also desirable

to use essentially the same digital interface device in systems which do not use the proprietary encryption system such as HDCP. Accordingly, in order to use the same physical hardware components to construct digital interface devices which can be permanently configured to allow or disallow use of a proprietary encryption scheme such as HDCP, the non-volatile RAM 26 of the digital interface device 20 of the present invention contains a specified write-protectable area 30 of preferably at least 512 bytes which operates as a write-once memory within the non-volatile RAM 26. Accordingly, the control circuitry 24 which controls the writing to the non-volatile RAM 26 is configured to check a specific flag address within the allocated write-once address area 30 of the non-volatile RAM 26. Preferably, a flag address check by the controller is conducted automatically on power up of the system and any reinitialization of the graphics controller. If the flag address contains a predetermined value, the specified address area within the non-volatile RAM 26 is write-protected and the controller 24 can only write information into other areas of the non-volatile RAM 26. In lieu of a single flag address, multiple addresses may be provided which are checked for a certain state or combination of states for write protection enablement.

Preferably, the specified area 30 for the encryption information is at the highest address range of the non-volatile RAM 26. For example, if a 64k byte non-volatile RAM is provided having addresses 0x0000 to 0xFFFF, a 1k byte area having addresses from 0xFC00 to 0xFFFF (63k to 64k-1) is designated as the specific write-protectable area 30 within the non-volatile RAM for encryption information. Preferably, the encryption key flag address is at the first byte of the specified area, i.e. preferably at 0xFC00 (63k).

The flag itself may have more than one predetermined value to render the entire specified area 30 as write-protected. For example, the interface device can be configured to recognized the ASCII character "H" as a write-protect flag which also indicates enablement of HDCP encryption and the storage of valid HDCP keys within the write-protected block. A value corresponding to ASCII "h" can be used to indicate write-protection, but that the HDCP encryption is disabled. If neither ASCII "H" or "h" is stored at the flag address, the allocated area would not be write-protected in such an

example. Preferably, however, only a single unique flag value is used for each different state, i.e. only "H" for the write protect HDCP encryption enabled state and "h" for write protect HDCP encryption disabled state.

Alternatively, the predetermined value may be inferentially set by specifying that the area 30 is write-protected if it contains any value other than, for example, an ASCII "W", thus, indicating the area 30 is writable. Preferably, the "W" value, if used, is initially stored at the flag address when the specified area 30 is allocated.

If the interface devices were shipped without a predetermined flag stored at the flag address to write-protect the specified area 30, the interface device could be subject to third party tampering. Accordingly, one of the final production step is preferably to either store encryption keys within the designated area 30 and set the flag address to "H" or set the flag address to "h" to disable HDCP encryption functions. Since royalties may be payable for creating devices which utilize encryption schemes such as HDCP, no royalties would be due with respect to interface devices where the encryption is permanently disabled.

By allocating the highest addresses 0xFC00 to 0xFFFF (63k to 64k-1) to the specified write-protectable area 30, the remainder of the non-volatile RAM at addresses 0x0000 to 0xFBFF (0k to 63k-1) is free to be used for the existing BIOS or any updated BIOS. Typical BIOS images range between 40 to 48k bytes. Accordingly, even if BIOS updates become larger in size, there is sufficient room within a 64k byte flash RAM to be accommodated since only the uppermost kilobyte of the flash RAM is used. If a 128K flash RAM is utilized, the write-protectable area 30 is preferably located at address range 0x1FC00 to 0x1FFFF (127k to 128k-1) with the flag address at 0x1FC00 (127k).

Before the flag is set, the specified write-protectable area 30 can be written into in a manner suitable for storing the encryption information. Preferably, the first four bytes of the area receive values corresponding to ASCII characters "H", "D", "C", "P", when the area is written to with encryption key data of the type usable by the HDCP encoding system. Preferably, the first thirteen bytes of the area 30 are written with values

corresponding to ASCII characters "h", "d", "c", "p", " ", "d", "i", "s", "a", "b", "l", "e", "d", when written to permanently disable HDCP encryption.

*　　　*　　　*

CLAIMS

What is claimed is:

1. A digital interface device for facilitating key encryption of a digital signal which is communicated from a computer system to an associated peripheral device, where the associated peripheral device decrypts the communicated digital signal for use, the interface device comprising:

a digital output;

digital output formatting circuitry associated with said output;

a non-volatile RAM for containing a BIOS for controlling digital output formatting having a specific write-protectable area allocated for storing an encryption key flag at a flag address and encryption key data; and

said specific write-protectable area being rendered read-only when a predetermined flag value is stored at said flag address whereby encryption key data may be stored in said specific area of said non-volatile RAM in connection with storing said predetermined flag value at said flag address such that stored encryption data cannot be altered by a subsequent write operation to said non-volatile RAM.

2. A digital interface device according to claim 1 configured to receive either a first predetermined flag value at said flag address in association with key encryption data in said specific write-protectable area which first flag value indicates encryption enablement.

3. A digital interface device according to claim 1 configured to receive either a first predetermined flag value at said flag address in association with key encryption data in said specific write-protectable area which first flag value indicates encryption enablement or a second predetermined flag value at said flag address which second flag value indicates encryption disablement in which case the digital interface device is permanently disabled from using the key encryption.

4. A digital interface device according to claim 1 configured to receive as said predetermined value any value other than a specific value which specific value enables writing into said write-protectable area.

5. A digital interface device according to claim 1 wherein said key flag is a combination of one or more values stored at the one or more flag addresses within said write protectable area.

6. A digital interface device according to claim 1 wherein the associated peripheral device is a digital display and said digital output is an output port for a digital video signal.

7. A digital interface device according to claim 6 which is configured as a digital video interface card.

8. A digital interface device according to claim 1 wherein said specific write-protectable area is at least 512k bytes and located at an address range higher than an address range reserved for a BIOS.

9. A method for producing digital interface devices comprising:

providing a digital interface device having a digital output, digital outport formatting circuitry associated with said output, and a non-volatile RAM for containing a BIOS for controlling digital output formatting;

allocating a specific addressable area on said non-volatile RAM for storing an encryption key flag and encryption key data; and

rendering said specific area read-only when a predetermined key flag value is written in said specific addressable area at a key flag address.

10. A method according to claim 9 further comprising:

writing a first predetermined flag value at said key flag address along with key encryption data in said specific area to enable key encryption.

11. A method according to claim 9 further comprising:

writing a first predetermined flag value at said key flag address along with key encryption data in said specific area to enable key encryption; or

writing a second predetermined flag value at said key flag address to permanently disable key encryption using said specific area.

12. A method according to claim 9 further comprising storing a specific value in said key flag address at the time the specific addressable area is allocated wherein said predetermined key value is any value other than said specific value.

ABSTRACT

A digital interface device is provided for facilitating key encryption of a digital signal which is communicated from a computer system to an associated peripheral device, such as a digital display device. The digital interface device has a digital output, digital output formatting circuitry associated with the output and a non-volatile RAM for storing a basic input/output system (BIOS) for, inter alia, controlling digital output formatting. The interface device is configured such that the non-volatile RAM has a specific addressable write-protectable area allocated for storing an encryption key flag at a flag address along with encryption key data. The write-protectable area is rendered read-only when a predetermined flag value is stored at the flag address. Thus, encryption key data may be stored in the specific write-protectable area of the non-volatile RAM in connection with storing the predetermined flag at that flag address such that encryption data cannot be altered when the flash RAM is subsequently written to, such as when a BIOS stored in the non-volatile RAM is updated.

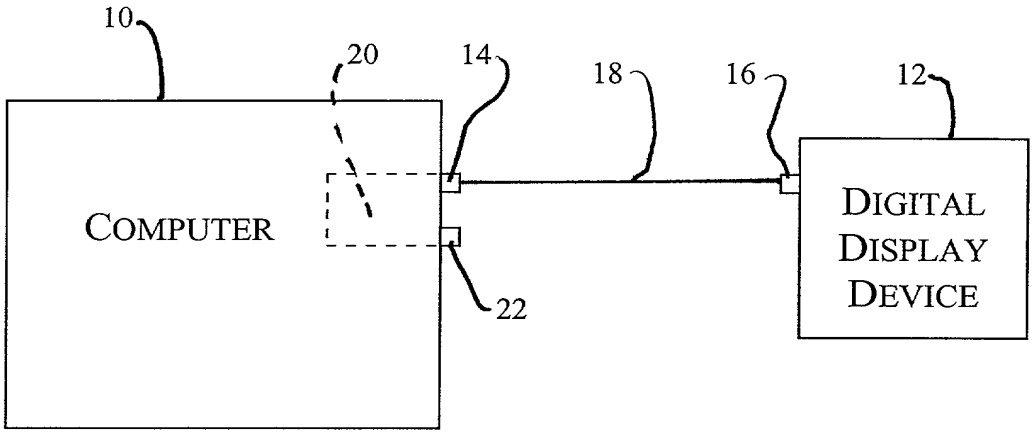
10
20
14
18
16
12
COMPUTER
22
DIGITAL
DISPLAY
DEVICE

FIG. 1

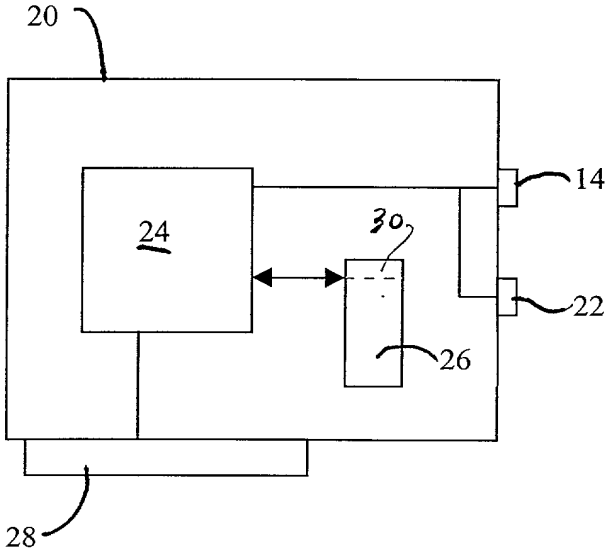
20
14
24
30
22
26
28

FIG. 2

Express Mail Label No. EL566349206US

Please type a plus sign (+) inside this box → [+]

PTO/SB/01 (12-97)
Approved for use through 9/30/00. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☒ Declaration Submitted with Initial Filing OR ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	ATI-000153BT
First Named Inventor	David I. J. Glen
COMPLETE IF KNOWN	
Application Number	Not Yet Known
Filing Date	Not Yet Known
Group Art Unit	Not Yet Known
Examiner Name	Not Yet Known

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

WRITE ONCE SYSTEM AND METHOD FOR FACILITATING DIGITAL ENCRYPTED TRANSMISSIONS

(Title of the Invention)

the specification of which

☒ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) _____ as United States Application Number or PCT International Application Number _____ and was amended on (MM/DD/YYYY) _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	
		☐ Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → [+]

PTO/SB/01 (12-97)
Approved for use through 9/30/00. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (If applicable)

☐ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: ☒ Customer Number 25310 → *Place Customer Number Bar Code Label here*

OR

☐ Registered practitioner(s) name/registration number listed below

Name	Registration Number	Name	Registration Number

☐ Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto.

Direct all correspondence to: ☒ Customer Number or Bar Code Label 25310 *OR* ☐ Correspondence address below

Name					
Address					
Address					
City		State		ZIP	
Country		Telephone		Fax	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])	Family Name or Surname
David I. J.	Glen

Inventor's Signature	[signature]					Date	Nov 1, 2000
Residence: City	Toronto	State	Ontario	Country	Canada	Citizenship	Canadian
Post Office Address	14 Glen Manor Drive						
Post Office Address							
City	Toronto	State	Ontario	ZIP	M4E 2X2	Country	Canada

☐ Additional inventors are being named on the ____supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto